Claims:

1. A proxy server for relaying communications between applications and for performing an additional process comprising:

a key manager for managing multiple keys used to generate a digital signature to be provided for a message document that is exchanged between said applications;

a signature key determiner for extracting said message document from a predetermined application, and for, based on said message document, determining a key used to provide a digital signature; and

a signature generator for providing a digital signature for said message document by using said key that is obtained from said key manager based on a determination made by said signature key determiner, and for transmitting said message document with said digital signature to a destination application.

2. The proxy server according to claim 1, wherein said key manager sets multiple key selection rules for obtaining said key, and only when said key selection rules are satisfied can said signature generator obtain said key.

3. The proxy server according to claim 2, wherein, when said key for generating a digital signature for said message document can not be obtained, said signature generator employs a replacement key that is defined in advance to provide a digital signature.

4. The proxy server according to claim 3, wherein, after said signature generator has provided a digital signature using said replacement key, when said acquisition condition that is determined for the original key based on said message document is satisfied to enable the acquisition of said original key, said signature generator again provides a digital signature using said original key.

5. The proxy server according to claim 1, further comprising:

a log manager for storing said message document with a digital signature provided by said signature generator, and for managing a log.

6. The proxy server according to claim 4, wherein said log manager stores not only said message document for which said signature generator has provided a digital signature using said replacement key, but also said message document without digital signature; and wherein said signature generator obtains, from said log manager, said message document without said digital signature, and provides a digital signature using said original key.

7. A digital signature system comprising:

applications for performing data processing; and

a proxy server connected to said applications via a network,

wherein said proxy server intercepts a communication, transmitted through said network, from an application to an

external destination device, provides a digital signature for a message document exchanged via said communication, and transmits said message document with said digital signature to said external destination device.

8. The digital signature system according to claim 7, wherein said proxy server permits a key used to provide a digital signature to be changed in accordance with the contents of a message document; and wherein said proxy server sets key selection rules for said key and permits digital signature using said key when said key selection rules have been satisfied.

9. The digital signature system according to claim 8, wherein, when said key selection rules for said key used to provide a digital signature for said message document have not been satisfied, said proxy server employs a predetermined replacement key to provide a digital signature; and wherein, when said key selection rules for said key are satisfied after said digital signature has been provided using said replacement key, said proxy server again employs said key to provide a digital signature for said message document.

10. A digital signature verification system comprising:

applications for performing data processing; and

a proxy server connected to said applications via a network,

wherein said proxy server intercepts a communication from an external destination device to an application

transmitted through said network, verifies a digital signature provided for a message document exchanged via said communication, and transmits said message document that has been authorized.

11. A network system comprising:

multiple groups connected to a wide area network, all of which have applications for performing data processing and proxy servers connected to said applications via a local area network,

wherein said proxy server intercepts a communication transmitted by an application of a local group to an application of a different group, provides a digital signature for a message document exchanged via said communication, and transmits said message document with said digital signature to said application of said different group, and

wherein said proxy server intercepts a communication from said application of said different group to said application of said local group, verifies a digital signature provided for a message document exchanged via said communication, and transmits said authorized message document to said application of said local group.

12. The network system according to claim 11, wherein, when said application of said local group transmits a message document, said proxy server stores the message document with a digital signature in a log, and manages said log; wherein, when said application of said local group receives a message document from a different group, said proxy server stores in

a log a message document authenticated by a verification of a digital signature, and manages said log; and wherein, at a predetermined timing, said proxy server compares the transmission log with the reception log for the same message document, and authorizes communication.

13. The network system according to claim 12, wherein said proxy server compares signature information for a digital signature concerning the same message document.

14. The network system according to claim 12, wherein said proxy server compares hash values used for providing a digital signature for the same message document.

15. A digital signature method comprising: providing a digital signature for a message document exchanged by applications and for authorizing said message document, including the steps of:

selecting, in accordance with the type of a message document transmitted by a predetermined application, a key used for providing a digital signature for said message document;

providing a digital signature for said message document, when key selection rules set for said key are not established, by using a replacement key that is set in advance for said key;

transmitting said message document with said digital signature to a destination designated by said application; and

using said key, when said key selection rules for said

key have been satisfied after said digital signature has been provided using said replacement key, to again provide a digital signature, and transmitting said message document with said digital signature to said destination.

16. A digital signature verification method comprising: for verifying a digital signature provided for a message document exchanged by applications, and for authorizing said message document, including the steps of:

accepting a message document with a digital signature that uses a replacement key, when said digital signature on said received message document has been provided by using said replacement key for an original key that is determined in accordance with the type of said message document;

receiving a message document, after said message document signed using said replacement key has been accepted, with a digital signature that used said original key; and

verifying a digital signature, provided using said original key, to authorize said message document with said digital signature that uses said replacement key.

17. A storage medium on which input means of a computer stores a computer-readable program that permits said computer to function as:

key management means for managing a key used to generate a digital signature to be provided for a message document that is exchanged between said applications;

signature key determination means for extracting said message document from a predetermined application, and for,

based on said message document, determining a key used to provide a digital signature; and

signature generation means for providing a digital signature for said message document by using said key that is obtained from said key management means based on a determination made by said signature key determination means.

18. A storage medium on which input means of a computer stores a computer-readable program that permits said computer to perform:

a process for selecting a key used to provide a digital signature for a message document in accordance with a type of message document transmitted from a predetermined application;

a process for providing said digital signature for said message document using said key that is selected, and for employing a predetermined replacement key to provide said digital signature for said message document, when key selection rules for said key used to provide a digital signature for said message document have not been satisfied; and

a process for employing said key to provide again a digital signature for said message document, when said key selection rules for said key are satisfied after said digital signature has been provided using said replacement key.

19. A program transmission apparatus comprising:

storage means for storing a program that permits a computer to function as:

key management means for managing a key used to generate a digital signature to be provided for a message document that is exchanged between said applications,

signature key determination means for extracting said message document from a predetermined application, and for determining a key used to provide a digital signature based on said message document, and

signature generation means for providing a digital signature for said message document by using said key that is obtained from said key management means based on a determination made by said signature key determination means; and

transmission means for reading said program from said storage means, and for transmitting said program.

20. A program transmission apparatus comprising:

storage means for storing a program that permits a computer to perform:

a process for selecting a key used to provide a digital signature for a message document, in accordance with the type of message document transmitted from a predetermined application,

a process for providing said digital signature for said message document using said key that is selected, and for employing a predetermined replacement key to provide said digital signature for said message document when key

selection rules for said key used to provide a digital signature for said message document have not been satisfied, and

a process for, when said key selection rules for said key are satisfied after said digital signature has been provided using said replacement key, employing said key to provide again a digital signature for said message document; and

transmission means for reading said program from said storage means, and for transmitting said program.

21. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing relaying communications between applications and performing an additional process, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 1.

22. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 7.

23. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for a digital signature verification system, the

computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 10.

24. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for a network system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 11.

25. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature method, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 15.

26. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature verification method, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 16.

27. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature method, said method steps comprising the steps of claim 15.

28. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature verification method, said method steps comprising the steps of claim 16.